Software and Digital Systems Safety (SDSS) Research Program

Leanna Rierson

May, 2002

1

Acronym List

- AACE — Airworthiness Assurance Center of Excellence
- ACR — Avionics Computer Resource
- ASU — Arizona State University
- ATM — Air Traffic Management
- AVSI — Aerospace Vehicle Systems Institute
- CNS — Communication, Navigation, and Surveillance
- COTS — Commercial-off-the-shelf
- FAA — Federal Aviation Administration
- FPGA — Field-Programmable Gate Array
- FY — Fiscal Year
- HUMS — Health Usage Monitoring System
- IMA — Integrated Modular Avionics

2

Acronym List (cont)

- MC/DC   Modified Condition/Decision Coverage
- NASA   National Aeronautics & Space Administration
- NJIT   New Jersey Institute of Technology
- OO   Object-oriented
- OS   Operating System
- RTOS   Real-Time Operating System
- SDSS   Software and Digital Systems Safety
- WAAS   Wide-Area Augmentation System

3

Briefing Outline

- SDSS Research Program Purpose
- SDSS Technical Community
- SDSS Research History
- SDSS Research Priorities
- Overview of SDSS Tasks

4

Leanna Rierson

SDSS Research Program Purpose

- To address safety, performance, and technology issues in the areas of:
  - Software
  - Complex electronic hardware
  - Digital systems
- SDSS research supports the policy and guidance initiatives of the FAA

5

SDSS Technical Community

- **Leader: Leanna Rierson**
- **Sponsor: Barbara Lingberg**
- **Tech Ctr Mgr: Chuck Kilgore**
- **Members:**
  - Will Struck
  - Jorge Castillo
  - Robin Sova
  - Gary Horan
  - Brenda Ocker
  - Dennis Wallace
  - John Lewis
  - Jim Treacy
  - Tony Lambreghts
  - Tom Kraft
  - Larry Bessette

6

SDSS Research History

- Past Research in the Areas of:
  - Modified Condition/Decision Coverage (MC/DC)
  - Service History
  - COTS Software
  - COTS Hardware
- See FAA Software Web-site for Reports:
  - http://av-info.faa.gov/software

7

SDSS Research Priorities

1- COTS software and components
2- Object oriented technology
3- Complex electronic hardware case study
4- Software development tools assessment
5- Software verification tools assessment
6- New paradigm for aircraft fly-by-wire control
7- Databus evaluation criteria
8- Semiconductor wearout effects
9- Tool qual of complex electronic hardware
10- Real-time scheduling analysis

8

Leanna Rierson

SDSS Priorities (cont)

11- Ethernet as an aviation databus
12- Avionics computer resource issues
13- Microprocessor evaluations
14- Safety engineering in software
15- Software service history and reliability models
16- Transfer of aviation data on the internet
17- COTS ground systems verification
18- Software service history case study

9

1. COTS Software

- Purpose: To evaluate COTS operating systems (OS), integration techniques, and protections schemes.
- Significance: A number of projects are attempting to use COTS OS's in aviation products.
- Status:
  - Phases 1 & 2 were carried out in FY01 by UTRC.
  - Phases 3 & 4 are currently underway with UTRC.

10

Leanna Rierson

FAA National Software Conference, May 2002
FAA Research Initiatives

2. Object-Oriented (OO) Technology

- Purpose: To identify and address OO issues in airborne software, particularly Level A software.
- Significance: A number of manufacturers are using OO design and programming techniques for Part 23, 25, 27, 29, & 33.
- Status:
  - Phase 1 is underway with NASA & Boeing
  - FAA/NASA held a workshop in April 2002
  - Phase 2 will likely begin in FY03

11

3. Complex Hardware Case Study

- Purpose: To carry-out a real-life field-programmable gate array (FPGA) design using RTCA/DO-254 and to identify areas for improvement.
- Significance: DO-254 is being invoked by the FAA for all classes of aircraft.
- Status: NASA Langley is in the final stages of this project.
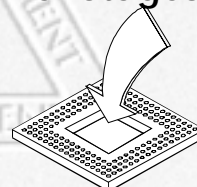
12

Leanna Rierson

4. Software Development Tools

- Purpose: To identify software development tool qualification issues and to propose solutions.
- Significance: Many manufacturers are proposing the use of autocode generators and other development tools.
- Status: Contract with Embry-Riddle recently awarded through FAA's Airworthiness Assurance Center of Excellence (AACE).

13

5. Software Verification Tools

- Purpose: To identify software verification tool qualification issues and to propose solutions.
- Significance: Nearly all airborne software projects use tools to satisfy some of the DO-178B objectives. Flight controls in particular are typically Level A and must have accurate tools. FAA and industry need evaluation criteria for verification tools.
- Status: Being started through NASA Langley.

14

Leanna Rierson

6. New Fly-By-Wire Paradigms

- Purpose: To evaluate possibility of adaptive controls on Part 23 aircraft.
- Significance: Could significantly improve the safety of general aviation.
- Status: Being carried out by Wichita State University via AACE.

15

7. Databus Evaluation Criteria

- Purpose: To evaluate a number of databuses and develop criteria for evaluation.
- Significance: Several "new" databuses are being proposed on biz jet projects (part 23 & 25).
- Status:
  - Not currently funded.
  - AACE project on Ethernet might address some of these concerns (ASU and Honeywell).
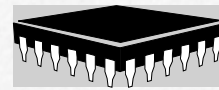
16

Leanna Rierson

8. Semiconductor Wearout

- Purpose: To identify and address effects of semiconductor wearout.
- Significance: All advanced avionics use semiconductors. They may wearout in 2-5 years. This affects all classes of aircraft and engines (part 23, 25, 27, 29, 33).
- Status:
  - Not currently funded.
  - Aerospace Vehicle Systems Institute (AVSI) is attempting to get something started.

17

9. Tool Qual of Complex Electronic Hardware Tools

- Purpose: To identify tool qual issues for complex hardware and propose solutions.
- Significance: A number of engine, engine control, aircraft, & avionics manufacturers will use tools to comply with DO-254. However, criteria for accepting tool experience and evaluating accuracy is unclear.
- Status: Not currently funded.

Leanna Rierson

10. Real-time Schedulers

- Purpose: To identify and address safety issues of real-time operating system schedulers.
- Significance: A number of avionics & engine control manufacturers are using real-time operating systems (RTOS) with real-time schedulers.
- Status:
  - Contract recently awarded to NJIT via AACE to address some of these concerns.

19

11. Ethernet as a Databus

- Purpose: To identify safety issues with Ethernet and to address them.
- Significance: Ethernet is being strongly supported by large aircraft manufacturers & their suppliers in new projects. Several safety concerns have already been identified.
- Status:
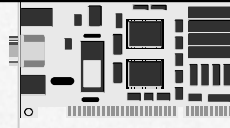 - Contract recently awarded to ASU and Honeywell via AACE.

20

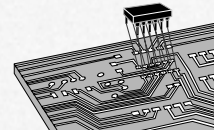Leanna Rierson

12. Avionics Computer Resource (ACR)

- Purpose: To identify ACR issues and propose solutions for safe implementation.
- Significance: ACR supports the new "Integrated Modular Avionics" (IMA) approach being proposed by many manufacturers.
- Status: Not currently funded.

21

13. Microprocessor Evaluation

- Purpose: To develop criteria for new microprocessor technology.
- Significance: All manufacturers are using new and more advanced microprocessors on their aircraft and engines. However, FAA does not have clearly defined criteria for acceptance.
- Status: Not currently funded. Hope to start in FY03.

22

Leanna Rierson

FAA National Software Conference, May 2002
FAA Research Initiatives

14. Safety Engineering in Software

- Purpose: To evaluate the safety assessment processes and their applicability in software assurance.
- Significance: Some manufacturers desire to use safety techniques to replace some of the RTCA/DO-178B objectives. However, there is currently no scientific evidence supporting this approach.
- Status: Not currently funded.

23

15. Software Service History and Reliability Models

- Purpose: To evaluate the applicability of reliability models in software assurance.
- Significance: Some manufacturers desire to use reliability models to support their service history claims.
- Status:
  - In FY01 a software service history handbook was created.
  - There is currently no funding for this phase of the effort.

24

Leanna Rierson

FAA National Software Conference, May 2002
FAA Research Initiatives

16. Transfer of Aviation Data on the Internet

- Purpose: To evaluate safety and security issues of transferring flight critical data via internet.
- Significance: Several manufacturers desire to transfer their flight software via internet to save time and expense.
- Status: Not currently funded.

25

17. COTS Ground Systems Verification

- Purpose: To evaluate COTS issues in support of health-usage monitoring system (HUMS) (e.g., safety, security, & integrity).
- Significance: HUMS is being implemented by several helicopter manufacturers. This project also helps support CNS/ATM initiatives.
- Status:
  - Contract recently awarded to ASU and UTRC via AACE.

26

Leanna Rierson

13

18. Software Service History Case Study

- Purpose: To use the WAAS program as a case study for software service history, using the newly developed handbook.

- Significance: WAAS plans to use service history. This project benefits the WAAS program, CNS/ATM implementation, and the airborne world.

- Status: Recently started through the WAAS program office via contract with Ferrell and Associates Consulting.

27

Related Research

- NASA's Aviation Safety Program
- Aerospace Vehicle Systems Institute (AVSI)
- Individual Companies
- Universities

28

Leanna Rierson

Summary

- Tasks Finishing Soon: 2, 3, 6
- Tasks Underway: 1, 4, 5, 10, 11, 17, 18
- Tasks Starting soon: 8, 13
- Stay posted to FAA software web-site for research reports
  - http://av-info.faa.gov/software
- Feel free to contact myself or Barbara Lingberg for further information.

29

Leanna Rierson